

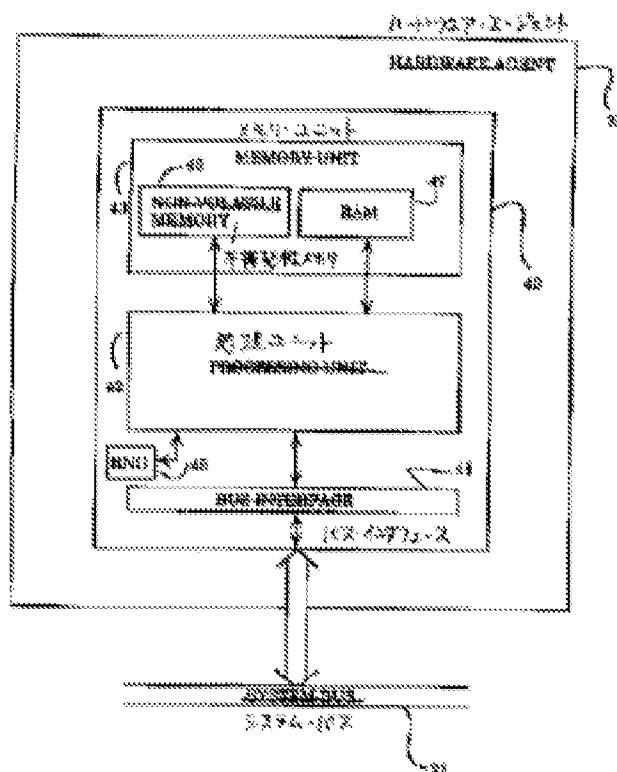
DEVICE AND METHOD FOR SECURITY COMMUNICATION

Patent number: JP9200194
Publication date: 1997-07-31
Inventor: DEREEKU ERU DEIBISU
Applicant: INTEL CORP
Classification:
 - international: **H04L9/08; G09C1/00; H04L9/10; H04L9/08; G09C1/00; H04L9/10;** (IPC1-7): H04L9/10; G09C1/00; H04L9/08
 - european:
Application number: JP19950353850 19951229
Priority number(s): JP19950353850 19951229

Report a data error here

Abstract of JP9200194

PROBLEM TO BE SOLVED: To reduce the danger of accidental disclosure of a public key/a private key in pairs against an illegal recipient by providing a storage means storing the keys in pairs and a digital certificate and a storage means storing processed information.
SOLUTION: A hardware agent 23 is made up of a single integrated circuit of a form of an enclosed die 40 and the die 40 is made up of a memory unit 43, and a picture unit 42 connecting to a bus interface 44 and a numeral generator 45. The bus interface allows communication from the hardware agent 23 to other device. Then the memory unit 43 includes a nonvolatile memory element 46 storing a public key/a private key in pairs and at least one digital certificate Moreover, the memory unit 43 includes a random access memory(RAM) 47 to store some results from the processing unit 42 and a corresponding algorithm.



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-200194

(43)公開日 平成9年(1997)7月31日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/10			H 0 4 L 9/00	6 2 1 A
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 Z
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 Z

審査請求 未請求 請求項の数 8 F D (全 15 頁)

(21)出願番号 特願平7-353850

(22)出願日 平成7年(1995)12月29日

(71)出願人 591003943

インテル・コーポレーション
 アメリカ合衆国 95052 カリフォルニア
 州・サンタクララ・ミッション カレッジ
 ブレーパード・2200

(72)発明者 デレーク・エル・デイビス

アメリカ合衆国 85044 アリゾナ州・フ
 ィニクス・イースト アシャースト ド
 ライブ・4129

(74)代理人 弁理士 山川 政樹

(54)【発明の名称】 安全保護の行われた通信を行うための装置および方法

(57)【要約】

【課題】 半導体デバイスと他の装置の間の安全保護された通信を確保する。

【解決手段】 デジタル証明書と組み合わせて暗号化とその解読キーを記憶する。半導体デバイスは暗号化とその解読キーと少なくとも1つのデジタル証明書を記憶するための不揮発性メモリと、他の装置および恐らくは暗号化とその解読アルゴリズムから半導体デバイスに入力された情報を一時的に記憶する内部メモリと、ハードウェア・エージェントに対して暗号化とその解読キーを完全に内部的に生成する乱数発生器とを備えている。

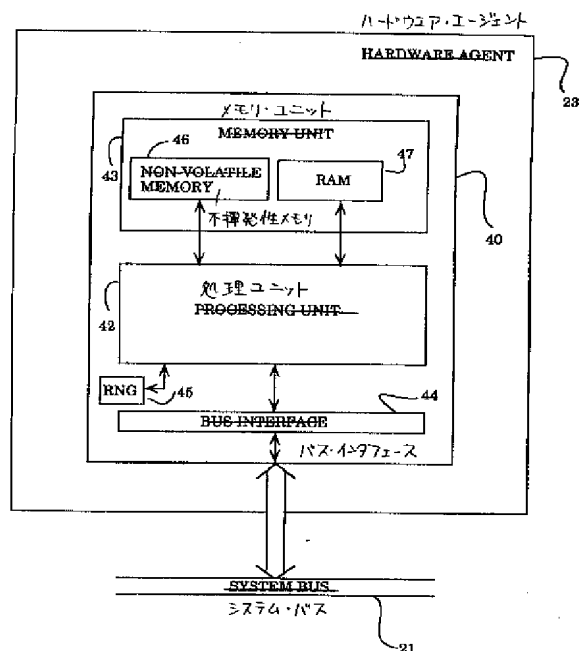


Figure 5

【特許請求の範囲】

【請求項1】 半導体デバイスにおいて、その半導体デバイス内の情報を処理する処理手段と、前記処理手段に結合され、独特に指定されたキー・ペアと少なくとも1つのデジタル証明書とを記憶する第1記憶手段と、前記処理手段に結合され、前記処理手段によって処理された前記情報を少なくとも記憶する第2記憶手段と、前記処理手段に結合され、前記半導体デバイスと第2の半導体デバイスの間の通信を可能とするインタフェース手段とを備えていることを特徴とする前記半導体デバイス。

【請求項2】 情報の符号化および復号化を行う半導体デバイスにおいて、独特に指定されたキー・ペアと少なくとも1つのデジタル証明書とを記憶する不揮発性メモリと、前記情報を記憶するランダム・アクセス・メモリと、前記不揮発性メモリと前記ランダム・アクセス・メモリとに結合され、前記情報を少なくとも内部的に処理する処理ユニットと、前記処理ユニットに結合され、前記半導体デバイスが少なくとも第2の半導体デバイスと通信を行うのを可能とするインタフェースとを備えていることを特徴とする前記半導体デバイス。

【請求項3】 前記の独特に指定されたキー・ペアを生成するための乱数発生器をさらに含んでおり、その乱数発生器が前記処理ユニットに結合されている請求項2に記載の半導体デバイス。

【請求項4】 少なくとも1つの暗号化／解読プログラムを記憶するメモリ手段と、前記暗号化とその解読プログラムを実行するホスト処理手段と、そのホスト処理手段と前記メモリ手段とを結合するバス手段と、そのバス手段に結合され、入力情報を内部的に解読し、出力情報を暗号化するエージェント手段とを備えており、そのエージェント手段が前記入力および出力情報を処理する処理手段と、前記処理手段に結合され、前記入力信号を解読し、前記出力信号を暗号化するために使用される独特に指定されたキー・ペアと少なくとも1つのデジタル証明書とを記憶する第1記憶手段と、少なくとも前記入力および出力情報を一時的に記憶する第2記憶手段と、前記処理手段に結合され、システムと遠隔システムとの安全保護された通信を可能とするインタフェース手段とを含んでいることを特徴とするシステム。

【請求項5】 少なくとも1つの暗号化とその解読プログラムを記憶するメモリ要素と、

前記暗号化とその解読プログラムを実行するためのホスト・プロセッサと、そのホスト・プロセッサと前記メモリ要素を結合するバスと、そのバスに結合され、遠隔装置からの入力情報を内部的に解読し、出力情報をその遠隔装置に伝送するために暗号化するハードウェア・エージェントを備えており、そのハードウェア・エージェントがハードウェア・エージェント内の前記入力および出力情報を処理するプロセッサと、前記プロセッサに結合され、両方とも前記入力情報の解読、および前記出力情報の暗号化に使用される独特に指定されたキー・ペアと装置証明書を記憶する不揮発性記憶要素と、前記入力および出力情報を一時的に記憶する揮発性記憶要素と、前記の独特に指定されたキー・ペアを生成する乱数発生器と、前記プロセッサに結合され、前記ハードウェア・エージェントと前記遠隔装置との間の安全保護された通信を可能とするインタフェースとを含んでいることを特徴とするシステム。

【請求項6】 他の遠隔装置との安全保護された通信を確実に行うために利用されるハードウェア・エージェントを作成する方法において、前記ハードウェア・エージェントが証明システムと電気的接続を確立するように前記ハードウェア・エージェントを前記証明システムに置くステップと、前記ハードウェア・エージェントにまず電力を供給し、前記ハードウェア・エージェント内の乱数発生器が装置固有のキー・ペアを生成する構成シーケンスを開始するステップと、前記の装置固有のキー・ペアが独特であることを検査するステップと、前記の装置固有のキー・ペアを前記ハードウェア・エージェント内の不揮発性記憶要素に記憶するステップとを備えていることを特徴とする前記方法。

【請求項7】 独特の装置証明書を作成するステップと、その装置証明書を前記ハードウェア・エージェントに入力するステップと、前記装置証明書を前記ハードウェア・エージェントの前記不揮発性記憶要素に記憶するステップとをさらに含んでいる請求項6に記載の方法。

【請求項8】 独特の第2レベル証明書を作成するステップと、その第2レベル証明書を前記ハードウェア・エージェントに入力するステップと、前記第2レベル証明書を前記ハードウェア・エージェントの前記不揮発性記憶要素に記憶する手段とをさらに含

んでいる請求項7に記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データ・セキュリティのための装置および方法に関する。詳細に言えば、本発明は製造時および／または製造後に暗号化とその解読キーを格納する半導体デバイスに関し、半導体デバイスを組み込んだシステムとそのシステムと遠隔通信を行う装置との間での安全保護された通信を確保するものである。

【0002】

【従来の技術】今日の社会においては、正当な受信者にとっては明確で曖昧なところがないが、不法な受信者には理解できない状態で、デジタル情報がある場所から他の場所へ伝送することがますます望まれるようになってきている。したがって、このような情報は通常、ある種の所定の暗号化アルゴリズムを実行するソフトウェア・アプリケーションによって暗号化し、暗号化された形態で正当な受信者へ伝送される。正当な受信者は伝送されてきた情報を解読して使用する。この暗号化とその解読伝送プロセスは一般に、政府で使用されており、また、機密情報を伝送する場合に、民間でも使用されている。

【0003】情報の暗号化とその解読が図1に示す対称キー暗号作成法によって達成されることがしばしばある。対称キー暗号作成法においては、同一のキー1（すなわち、一般に「対称キー」と呼ばれるデータ・ストリング）を正当な送信者2と正当な受信者3の両方が使用して、送信者2と受信者3の間で伝送されるメッセージ4（すなわち、情報）の暗号化および解読を行っている。このような暗号化および解読はRAS、DESなどの従来からある周知のアルゴリズムによって行われ、在来のネットワーク、電話回線などの公共施設を通じて、暗号化された形態で伝送が行われる。

【0004】対称キー暗号作成法は演算自体の面で単純なものであるが、複雑なキーの管理を必要とする。基本的に、各送信者は正当な各受信者との通信に異なる対称キーを必要とし、これにより、多数の従業員のいる企業で使用するのが、不可能とはいえないにしても困難となる。たとえば、1000の正当なエンティティ（たとえば、従業員）のある企業においては、各正当なエンティティが企業内の他のエンティティと通信できる場合、最大限499,500（ $1000 \times 99 / 2$ ）個のキーを管理する必要がある。さらに、対称キーを正当な送信者2から正当な受信者3へ伝送する確実で、便利な方法がないため、対称キー暗号作成法をネットワークや大域環境で実施するのは困難である。

【0005】他の暗号化とその解読方法は2つの別々のキー（「キー・ペア」と呼ぶ）を使用するものであり、図2に示すように、キー・ペアのうち第1のキー（「公開キー」）10は正当な送信者13からのメッセージ1

2の暗号化に使用され、キー・ペアのうち第2のキー（「私用キー」）11は正当な受信者14によるメッセージ12の解読に使用される。この方法は一般に「非対称」（または、公開）キー暗号作成法と呼ばれている。非対称キー暗号作成法の利点の1つは、対称キー暗号作成法に関連するわずらわしいキー管理の問題を軽減することである。上記の例について説明を続けると、非対称暗号化作成法に必要なキー・ペアの数は1000、すなわち正当なエンティティの総数に等しい。しかしながら、このような通信システムにおいては、不法なエンティティ（たとえば、産業スパイ）が業務の流れを混乱させたり、機密情報を入手することを目的として、偽のメッセージを他の正当なエンティティに送ることによって、正当なエンティティ（たとえば、従業員、合弁事業会社）を装うと試みることがある。それ故、付加的なプロトコルを非対称キー・システムに使用して、メッセージと発信者の認証を行うのが普通である。

【0006】発信者の認証（すなわち、公開キーの発信者が実際に公開キーの真の所有者であることを確認する）は、通信をそれまで未知の当事者の間で初めて確立するときに問題となる。この問題は一般に、図3に示すように、送信メッセージ12内にデジタル証明書15を組み込むことによって回避される。デジタル証明書15は相互に信任した機関16（たとえば、銀行、政府機関、業者団体など）によって発行されるもので、他人の公開キー10を使用しようという不正を試みても、判読できないメッセージがもたらされるだけとなる。このような相互信任機関16は関与する当事者によって異なっている。たとえば、同一の企業に雇用されている2人の人間はその企業の社内セキュリティ・オフィスが発行した証明書を両者ともに信用することとなる。2つの独立した企業の従業員は、しかしながら、それぞれの会社のセキュリティ・オフィスの証明書だけでなく、たとえば、このような企業エンティティの証明を行う業界団体の証明書も必要とすることになろう。このデジタル証明機関16による方法は公開キー10をエンティティ（たとえば、従業員）に「拘束」するものである。

【0007】ここ数年間に、「キー」情報が無許可の人間に取得されることを防止する多くの方式が出てきている。このような方式の1つは、特に盗難が容易なポータブル・コンピュータ用に機械的なセキュリティ機構を用いるものである。たとえば、いくつかの会社はラップトップのケースを許可なく開いた場合にキー資料を消去する不法行為検出機構を使用したラップトップを発表している。しかしながら、機械的なセキュリティ装置には、いくつかの関連した欠点がある。

【0008】機械的セキュリティ装置に関連した主な欠点は、これらをリバース・エンジニアリングによってごまかせることがあることである。他の欠点は、機械的なセキュリティ機構を設計し、製造することは費用がかか

るということである。また他の欠点はキー情報が偶発的に消去される可能性があることである。

【0009】結果として、多くの会社は暗号化とその解読プロトコルを使用したソフトウェア・アプリケーションだけに依存することとなっている。しかしながら、技術が迅速に発展するにともない、これらの暗号化とその解読ソフトウェア・アプリケーションは、情報の暗号化および解読速度が命令の実行速度に相関しているため、通信システムの伝送速度に不必要な制限を課すものとなる。

【0010】特定のハードウェアを顧客のシステムに用いて、このようなキーを開示から保護するというこの方式は、急速に成長している「コンテンツ流通」、すなわち情報の電子的な流通の分野でも使用されている。周知のコンテンツ流通システムの中には、(i)モデムその他の電子的手段によってソフトウェアを販売するもの、(ii)コンパクト・ディスク(「CD」)によって配布された情報の一部を販売するものなどがある。このような電子的な販売は関連する特定のデータを「復号」するための解読キーに依存している。たとえば、顧客は暗号化されたデータの多くのファイルを取めているCDに自由にアクセスできるが、特定のファイルを購入するには、そのファイルに対応した「解読キー」を購入しなければならない。しかしながら、キーを保護するために特定のハードウェアを使用する際の主な問題は、このようなハードウェアが無許可の使用の可能性をなくするために、情報の供給業者による完全な管理および統制を必要とすることである。

【0011】

【発明が解決しようとする課題】上記したところに基づき、少なくとも処理ユニットと、公開／私用キー・ペアを製造時に、また半導体デバイスを組み込んだシステムと他の遠隔システムの間で安全保護がより確実に行われる通信をもたらすための少なくとも1つのデジタル証明書を製造時および／またはそれ以降に記憶するための不揮発性メモリ要素とを有する半導体デバイスを開発することが望ましい。したがって、本発明の目的は、不法な受信者に対する公開／私用キー・ペアの偶発的開示の危険性をかなり減じる半導体デバイスを提供することである。

【0012】本発明の他の目的は、独特の公開／私用キー・ペアを内部で生成できる半導体デバイスを提供することである。

【0013】本発明のさらに他の目的は、安全保護のなされていない半導体デバイス外での私用キーの使用を防止するために私用キーを記憶する半導体デバイスを提供することである。

【0014】本発明のさらにまた他の目的は、リバース・エンジニアリングによるキー・ペアの検出を実質的に防止するために集積回路内での公開／私用キー・ペアの

記憶および使用に対して安全保護を施す半導体デバイスを提供することである。

【0015】本発明の他の目的は、デバイスを遠隔(電子的に)認証し、個々のユニットを識別するための独特のデジタル証明書を記憶する半導体デバイスを提供することである。

【0016】本発明の他の目的は、独特性および自己認証という機能により、遠隔エンティティ(コンテンツ流通業者など)に代わって補償された職務を遂行できる装置を提供することである。

【0017】本発明の他の目的は、データ通信および記憶のための費用効果の高い装置を提供することである。

【0018】

【課題を解決するための手段】半導体デバイスは、識別のための操作を行う処理ユニットと、独特の公開／私用キー・ペア、ならびにキー・ペアの真性を確認する少なくとも1つのデジタル証明書を記憶するための少なくとも1つの不揮発性メモリと、暗号作成アルゴリズムを記憶するためのメモリと、一時データを記憶するための揮発性ランダム・アクセス・メモリとを備えたハードウェア・エージェントである。ハードウェア・エージェントはさらに、他の装置との情報(暗号化または解読された)の送受信のためのインタフェースを含んでいる。

【0019】本発明の目的、特徴および利点は本発明に関する以下の詳細な説明から明らかとなろう。

【0020】

【発明の実施の形態】本発明は公開／私用キー・ペアおよび少なくとも1つのデジタル証明書をハードウェア・エージェント自体内に安全に記憶し、かつ使用することを対象としたハードウェア・エージェントおよびこれに関連した操作方法に関する。このデジタル証明書は装置の正当性を表す装置の製造業者が与えるデジタル証明書である「装置証明書」と、信任された第三者によるデジタル証明書である「第2レベル証明書」とを含んでいても、あるいは両方の証明書を集めたものを含んでいてもよい。以下の説明において、本発明を完全に理解させるためハードウェア・エージェントのいくつかの構成要素などのさまざまな細部が記載されている。しかしながら、当分野の技術者には、これらの細部が本発明の実施に必要ではないことが明らかであろう。場合によっては、本発明を不要に曖昧なものとしないうために、周知の回路、要素などの詳細を記載しない。

【0021】図4を参照すると、本発明を利用するコンピュータ・システム20が示されている。コンピュータ・システム20は少なくとも1つのホスト・プロセッサ22とハードウェア・エージェント23を含む複数のバス・エージェントの間で情報を通信することを可能とするシステム・バス21を含んでいる。Intel(登録商標)アーキテクチャのプロセッサであることが好ましいが、これに限定されるものではないホスト・プロセッ

サ22はプロセッサ・バス・インタフェース24を介してシステム・バス21に結合されている。本実施形態にはホスト・プロセッサ22だけしか示されていないが、複数のプロセッサをコンピュータ・システム20内に用いることも考えられている。

【0022】図4にさらに示すように、システム・バス21はメモリ・サブシステム25および入出力(I/O)サブシステム26へアクセスできるようにする。メモリ・サブシステム25はシステム・バス21に結合されたメモリ・コントローラ27を含んでおり、ダイナミック・ランダム・アクセス・メモリ(「DRAM」)、読取り専用メモリ(「ROM」)、ビデオ・ランダム・アクセス・メモリ(「VRAM」)などの少なくとも1つのメモリ装置に対するアクセスを制御するインタフェースをもたらす。メモリ装置28はホスト・プロセッサ22用の情報および命令を記憶している。

【0023】I/Oサブシステム26は、システム・バス21および従来のI/Oバス30に結合されたI/Oコントローラ29を含んでいる。I/Oコントローラ29はI/Oバス30とシステム・バス21の間のインタフェースであり、システム・バス21またはI/Oバス30上の装置が情報を交換するのを可能とする通信経路(すなわち、ゲートウェイ)をもたらす。I/Oバス30は、画像を表示するための表示装置31(たとえば、陰極線管、液晶表示装置など)、ホスト・プロセッサ22に対して情報およびコマンドの選択を伝えるための英数字入力装置32(たとえば、英数字キーボードなど)、カーソルの運動を制御するためのカーソル制御装置33(たとえば、マウス、トラックボールなど)、情報および命令を記憶するための大容量記憶装置34(たとえば、磁気テープ、ハード・ディスク装置、フロッピー・ディスク装置など)、コンピュータ・システム20と他の装置の間で情報を送受信するための情報送受信機35(ファックス装置、モデム、スキャナなど)、および情報の有形な視覚的表示をもたらすハード・コピー装置36(たとえば、プロッタ、プリンタなど)を含んでいるが、これらに限定されるものではないコンピュータ・システム20の少なくとも1つの周辺装置との間で情報を通信する。図4に示したコンピュータ・システムがこれらの構成要素のあるものまたはすべて、あるいは図示のものとは異なる構成要素を用いることができると考えることができる。

【0024】図5に示すような本発明の実施形態を参照すると、ハードウェア・エージェント23はホスト・プロセッサ22との通信経路を確立するためにシステム・バス21に結合されている。ハードウェア・エージェント23は半導体デバイス・パッケージ内に、好ましくは気密に、封入されたダイ40(たとえば、マイクロコントローラ)の形態の単一の集積回路からなっており、ダイ40を損傷および有害な汚染物から保護している。ダ

イ40はメモリ・ユニット43、バス・インタフェース44および数値発生器45に結合された処理ユニット42からなっている。バス・インタフェース44はハードウェア・エージェント23から他の装置(たとえば、ホスト・プロセッサ22)への通信を可能とする。処理ユニット42はダイ40内の安全保護環境内で計算を行って、許可を受けた受信者との有効な接続を確認する。このような計算には、ある種のアルゴリズムおよびプロトコルの実行、装置固有の公開/私用キー・ペアなどを発生するための回路(たとえば、本質的に乱数であることが好ましい数値発生器45)の活動化などがある。処理ユニット42は、私用キーを取得するためにコンピュータ・システムを混乱させる一般的な方法であるウィルスの攻撃による私用キーのアクセスを防止するため、ダイ40内に配置されている。

【0025】メモリ・ユニット43は公開/私用キー・ペアおよび少なくとも1つのデジタル証明書を記憶する不揮発性メモリ要素46を含んでいる。供給電力が停止したときに内容を保持するので、不揮発性メモリ46が使用される。メモリ・ユニット43は処理ユニット42および該当するアルゴリズムからのある種の結果を記憶するためにランダム・アクセス・メモリ(「RAM」)47をさらに含んでいる。

【0026】ハードウェア・エージェント23はセキュリティを高めるためシステム・バス21の周辺装置として実現されているが、ハードウェア・エージェント23をPCプラットフォーム・レベルで、たとえば、ハード・ディスクに対して入出力される情報を自動的に解読および/または暗号化するためのディスク・コントローラまたはPCMCIAカードなどのいくつかの他の態様で実施することも考えられる。他の代替実施形態はハードウェア・エージェント23を以下で説明するようなホスト・プロセッサ22を含むマルチチップ・モジュールの構成要素の1つとすることである。さらに、ハードウェア・エージェント23をPCプラットフォームに関連して説明するが、このようなハードウェア・エージェント23をファックス装置、プリンタなどの任意の入出力(「I/O」)周辺装置内で、あるいはコンピュータとI/O周辺装置の間の通信経路上で実施することも考えられる。

【0027】図6を参照すると、本発明を製造するための操作の流れ図が示されている。まず、ステップ100において、ハードウェア・エージェントのダイが従来の周知の半導体製造技法にしたがって製造される。次に、ダイを半導体パッケージ内に封入して、ハードウェア・エージェント自体を形成する(ステップ105)。ハードウェア・エージェントを、ハードウェア・エージェントと証明システムへの電気的接続を確立する証明システムに入れる(ステップ110)。証明システムは基本的に、ハードウェア・エージェントの証明のための電気信

号を発生し、受け取るための、プリント回路ボードに結合された担持体である。証明システムは独特のキーの生成を保証するために以前に生成された公開キーを記憶するための装置（たとえば、データベース）を含んでいる。次いで、証明システムはハードウェア・エージェントに電力を供給して、構成手順を開始する。この手順の間、乱数発生器は装置固有の公開／私用キー・ペアをハードウェア・エージェント内部で生成する（ステップ115）。

【0028】公開／私用キー・ペアの公開キーは証明システムに対して出力され（ステップ120）、以前に製造されたハードウェア・エージェントからの以前に生成された公開キーの記憶装置と比較される（ステップ125）。公開キーが以前に生成された公開キーと同一であるというきわめて起こりにくい状況においては（ステップ130）、ハードウェア・エージェントに他のこのような公開／私用キー・ペアを生成するようにという通知が証明システムによって行われ（ステップ135）、ステップ120のプロセスを継続する。このプロセスは各公開／私用キー・ペアが独特のものであることを確実とするものである。以前に生成された公開キーの記憶装置はこの新しい独特の公開キーによって更新される（ステップ140）。その後、ステップ145において、証明システムは製造業者の秘密の私用キーを用いて公開キーに「デジタル署名」する（一般的な言い方をすれば、製造業者の私用キーを用いて公開キーを暗号化することによって、独特の装置証明書を作成する。この証明書はハードウェア・エージェントに入力され（ステップ150）、ハードウェア・エージェントは独特の公開／私用キー・ペアおよび装置証明書を不揮発性メモリに永続的にプログラムする（ステップ155）。この時点で、装置は物理的に独特のものとなり、その真性性をもたすことができる。

【0029】図7を参照すると、ハードウェア・エージェントの遠隔検証の流れ図が示されている。ステップ200において、ハードウェア・エージェントが組み込まれたシステム（「ハードウェア・エージェント・システム」と遠隔システムとの間に通信リンクが確立される。遠隔システムとは、たとえば、他のハードウェア・エージェントが組み込まれていたり、あるいはハードウェア・エージェントと通信するソフトウェアを実行するシステムである。ハードウェア・エージェントはその独特の装置証明書を遠隔システムに対して出力する（ステップ205）。製造業者の公開キーが公開されており、一般に入手できるものであるため、遠隔システムは装置証明書を解読して、ハードウェア・エージェントの公開キーを取得する（ステップ210）。

【0030】その後、ステップ215において、遠隔システムはランダムな呼掛け（すなわち、テスト用のデータ・シーケンス）を生成し、これをハードウェア・エー

ジェント・システムに伝送する（ステップ220）。ステップ225において、ハードウェア・エージェントは応答を生成し（すなわち、ハードウェア・エージェントの私用キーを用いて呼掛けを暗号化し）、これを遠隔システムへ伝送する（ステップ230）。次いで、遠隔システムはハードウェア・エージェントから伝送された装置証明書から予め決定したハードウェア・エージェントの公開キーを使用して応答を解読する（ステップ235）。ステップ240において、遠隔システムは元の呼掛けを解読した応答と比較し、同一であれば、システムと遠隔システム間の通信は安全であり、維持される（ステップ245）。それ以外の場合、通信は打ち切られる（ステップ250）。この時点で、遠隔システムには、特定の製造業者が製造した特定の装置（既知の特性の）と直接更新していることが保証される。ここで、遠隔システムはハードウェア・エージェントに遠隔システムに代わってターゲット・システム内で特定の機能を実行するよう指示することができる。これらの機能の整合性および関連するデータの機密性が保証される。このような機能にはコンテンツ流通キーの受信および使用、ならびに会計情報の維持などがある。

【0031】他の情報提供装置とともにコンテンツの流通が出現したこととともない、ハードウェア・エージェントが偽物ではないことの付加的な確認を与えるのが必要となる可能性がある。これはハードウェア・エージェントを含む半導体デバイスを、たとえば政府機関、銀行、業界団体などの信頼できる第三者エンティティに送ることによって達成できる。上述したのと同じ態様で、第三者エンティティの独特の第三者デジタル証明書（「第2レベル証明書」）がハードウェア・エージェントに入力される。その後、ハードウェア・エージェントは第2レベル証明書を公開／使用キー・ペアおよび恐らくは装置証明書とともに不揮発性メモリに永続的にプログラムする。結果として、ハードウェア・エージェントは装置証明書および第2レベル証明書の両方によって確認され、ハードウェア・エージェントの妥当性が保証され、ハードウェア・エージェントの不正な製造が防止され、第三者エンティティとハードウェア・エージェントの製造業者による、行われるとは思われない共謀が防がれる。

【0032】図8を参照すると、第2レベル証明書を使用した認証を含むハードウェア・エージェントの遠隔検証の流れ図が示されている。ステップ300において、通信リンクがハードウェア・エージェント・システムと遠隔システムの間で確立される。ハードウェア・エージェントはその独特の装置証明書と第2レベル証明書を遠隔システムに対して出力する（ステップ305）。次に、遠隔システムは製造業者が公表している公開キーを使用して装置証明書を解読し、ハードウェア・エージェントの公開キーを取得する（ステップ310）。同様

に、遠隔システムは第三者の完全に公表されている公開キーを使用して、ハードウェア・エージェントに記憶されているハードウェア・エージェントの公開キーを取得する(ステップ315)。

【0033】その後、ハードウェア・エージェントの2つのバージョンの公開キーが比較され(ステップ320)、2つのバージョンが同一でない場合には、通信が打ち切られる(ステップ325)。しかしながら、2つのバージョンが同一の場合には、遠隔システムはランダムな呼掛けを生成し、これをハードウェア・エージェントに伝送する(ステップ330)。ハードウェア・エージェントは応答、すなわちハードウェア・エージェントの私用キーを用いて暗号化した呼掛けを生成し(ステップ335)、これを遠隔システムに伝送する(ステップ340)。遠隔システムは次いで、ハードウェア・エージェントから予め伝送されているハードウェア・エージェントの公開キーを用いて応答を解読する(ステップ345)。ステップ350におけるように、遠隔システムは元の呼掛けを解読した応答と比較し、同一であれば、システムと遠隔システム間の通信は安全であり、維持される(ステップ355)。それ以外の場合には、通信が打ち切られる(ステップ360)。

【0034】本発明を多くの異なる方法で、かつ多くの異なる構成を使用して設計することができる。本発明をさまざまな実施形態によって説明したが、本発明の精神および範囲を逸脱することなく、他の実施形態が当分野の技術者には思い浮かべられるであろう。したがって、本発明は特許請求の範囲だけによって判断されるべきである。

【図面の簡単な説明】

【図1】従来の対称キー暗号化および解読プロセスを説

明するブロック図である。

【図2】従来の非対称キー暗号化および解読プロセスを説明するブロック図である。

【図3】信任された機関によるデジタル証明プロセスを説明するブロック図である。

【図4】本発明の実施形態を組み込んだコンピュータ・システムのブロック図である。

【図5】本発明の実施形態のブロック図である。

【図6】キー・ペアおよびデジタル証明書を半導体デバイスで実施する方法を説明する流れ図である。

【図7】ハードウェア・エージェントの作動を説明する流れ図である。

【図8】第2レベルの証明を使用したハードウェア・エージェントの遠隔検証を説明する流れ図である。

【符号の説明】

- 20 コンピュータ・システム
- 21 システム・バス
- 22 ホスト・プロセッサ
- 23 ハードウェア・エージェント
- 25 メモリ・サブシステム
- 26 I/Oサブシステム
- 27 メモリ・コントローラ
- 28 メモリ装置
- 40 ダイ
- 41 半導体デバイス・パッケージ
- 42 処理ユニット
- 43 メモリ・ユニット
- 44 バス・インタフェース
- 45 数値発生器
- 46 不揮発性メモリ要素
- 47 ランダム・アクセス・メモリ

【図1】

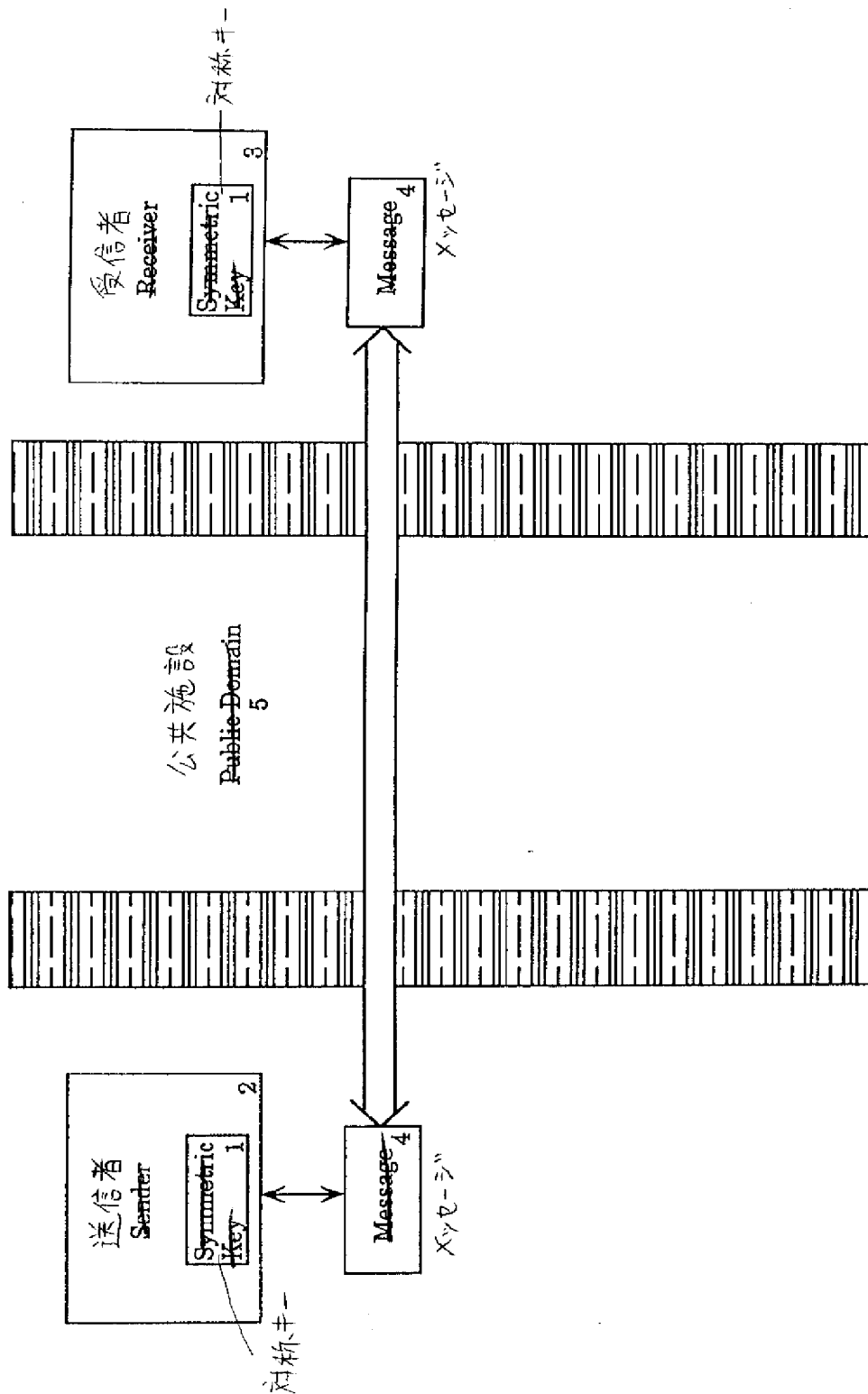


Figure-1

【図2】

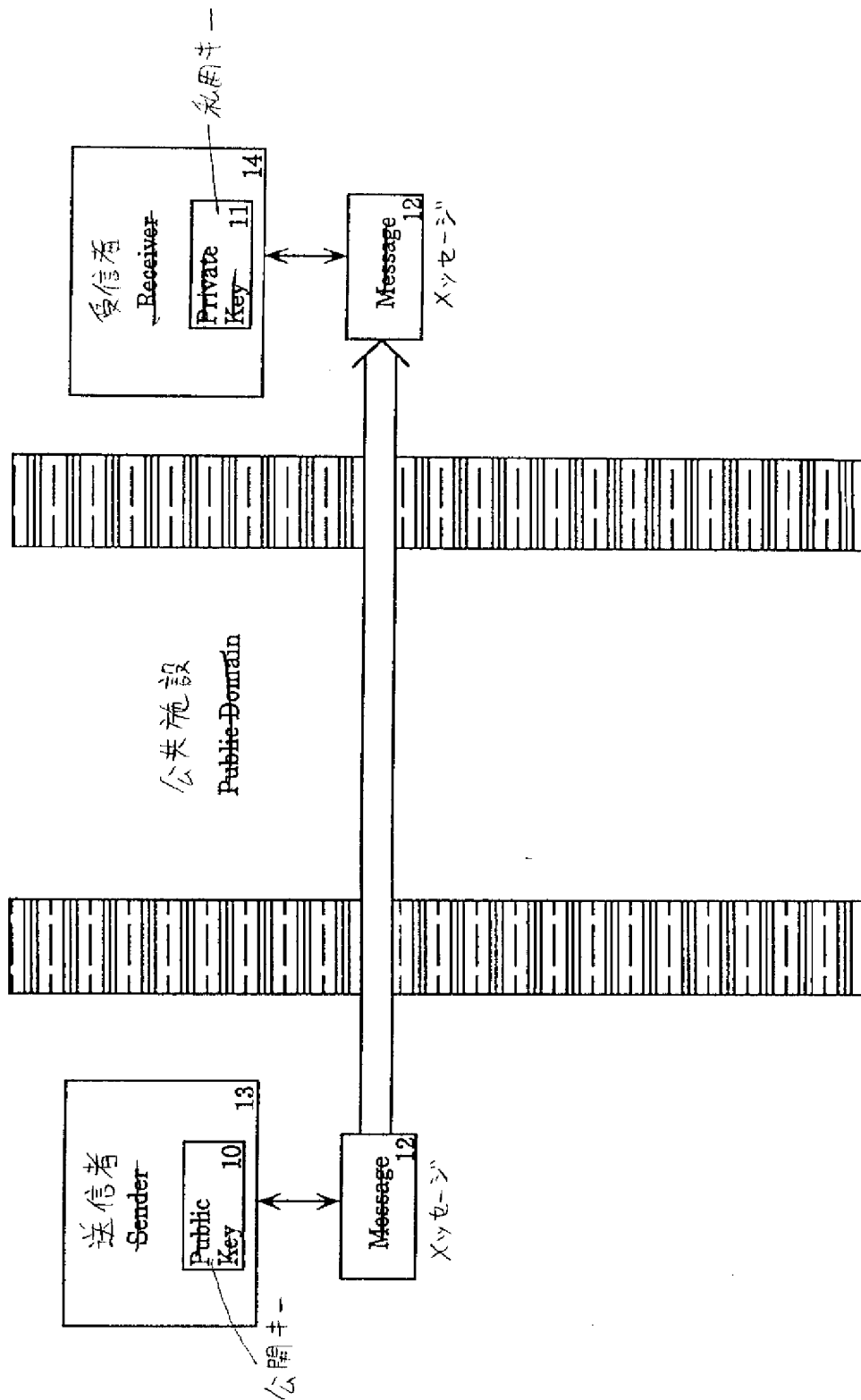


Figure 2

【図3】

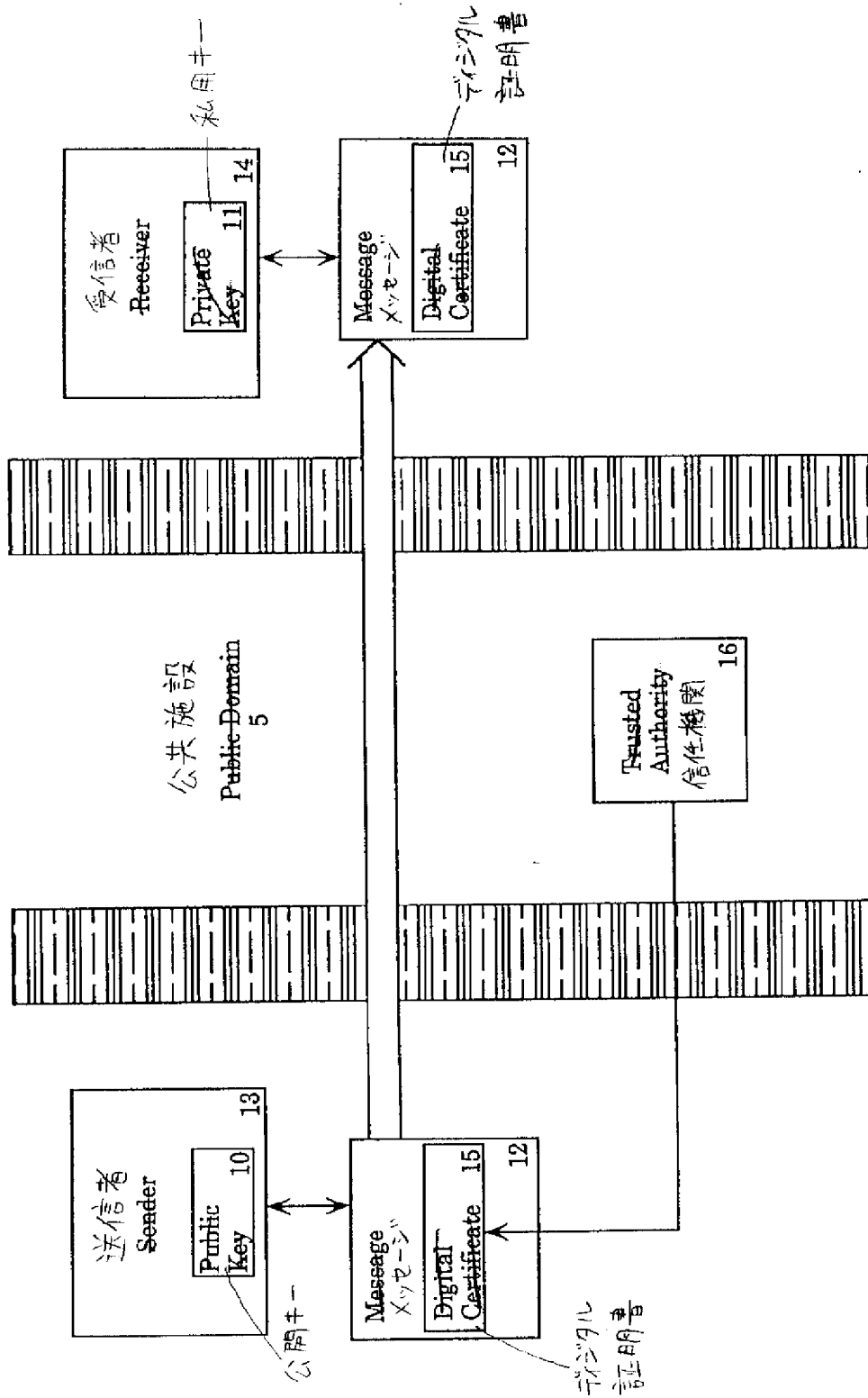


Figure 3

【図4】

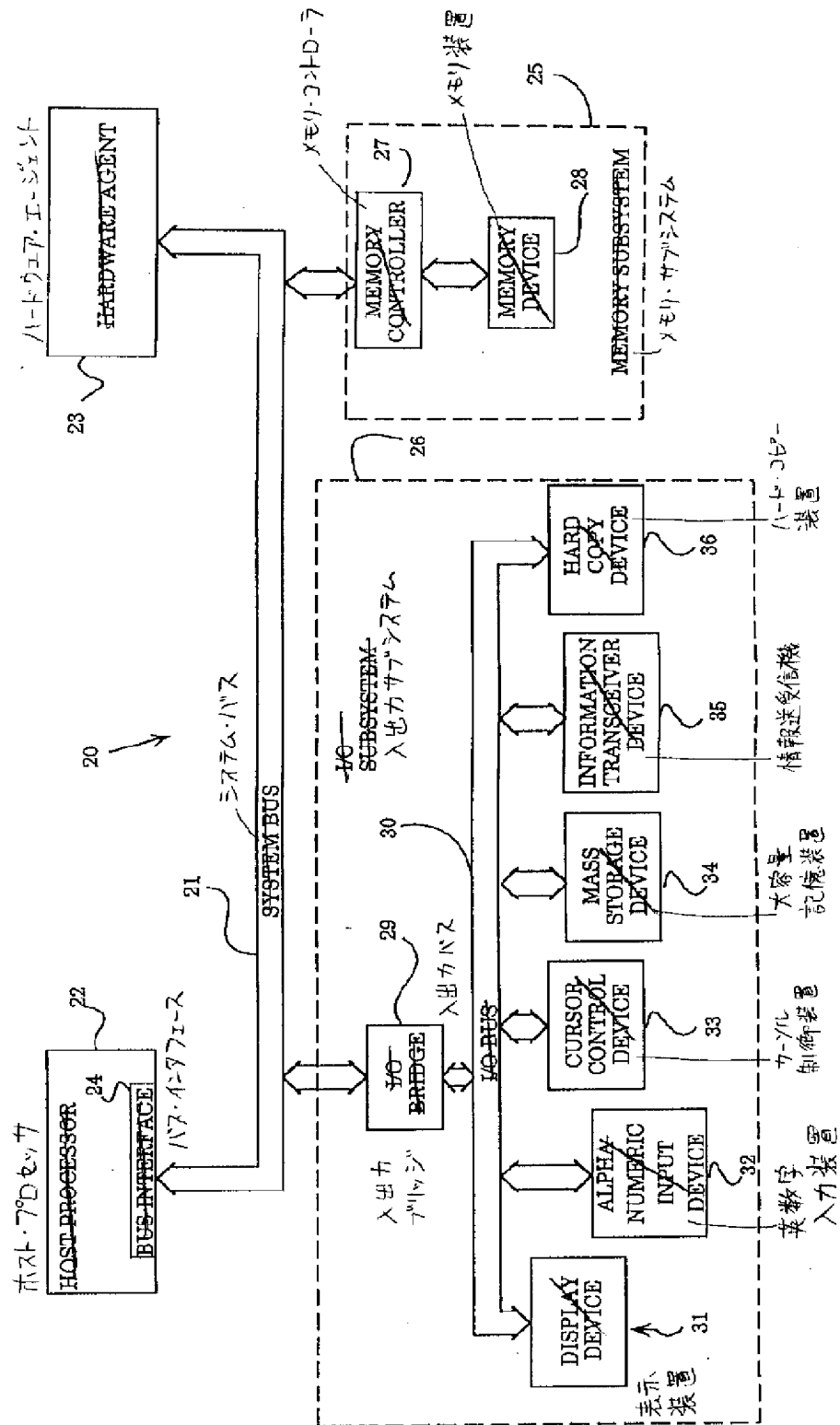
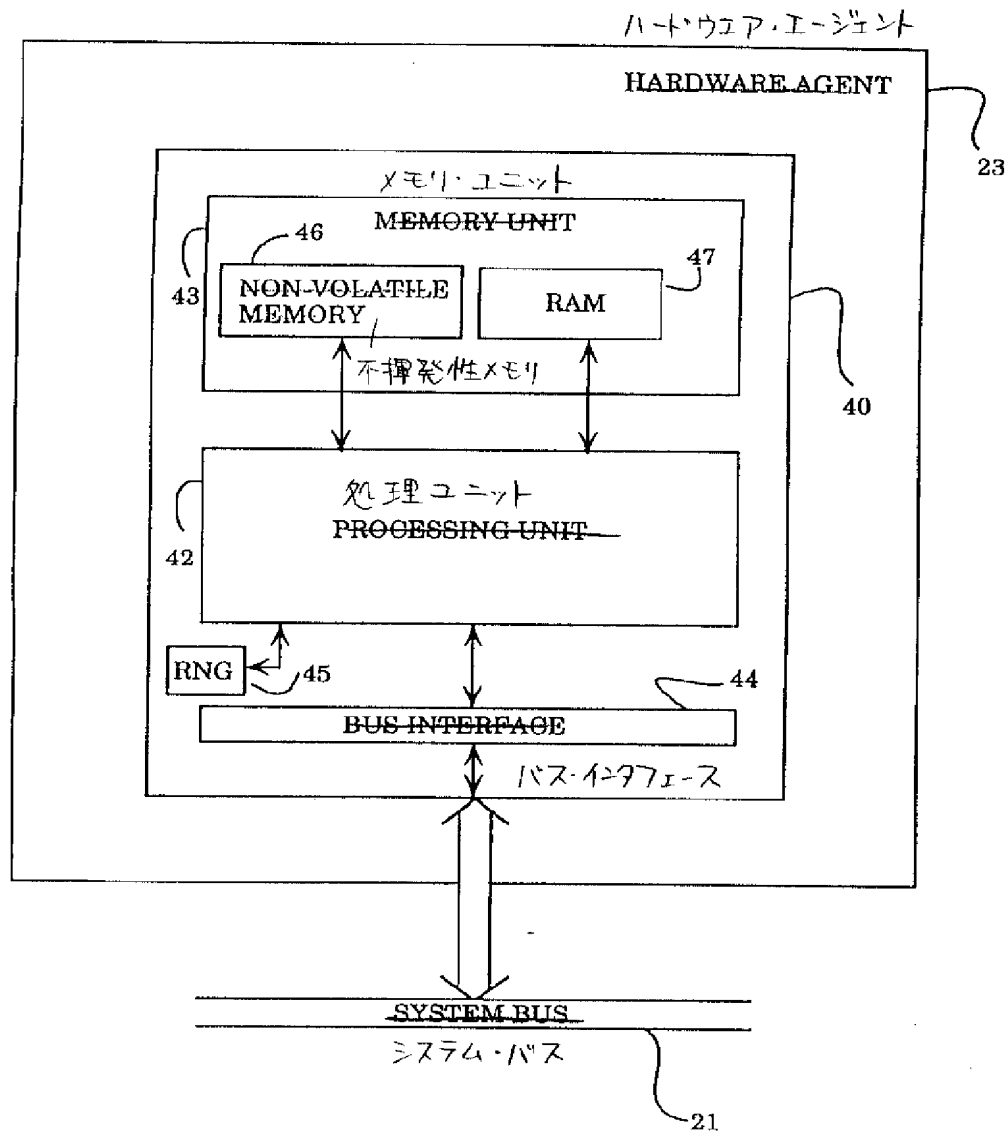
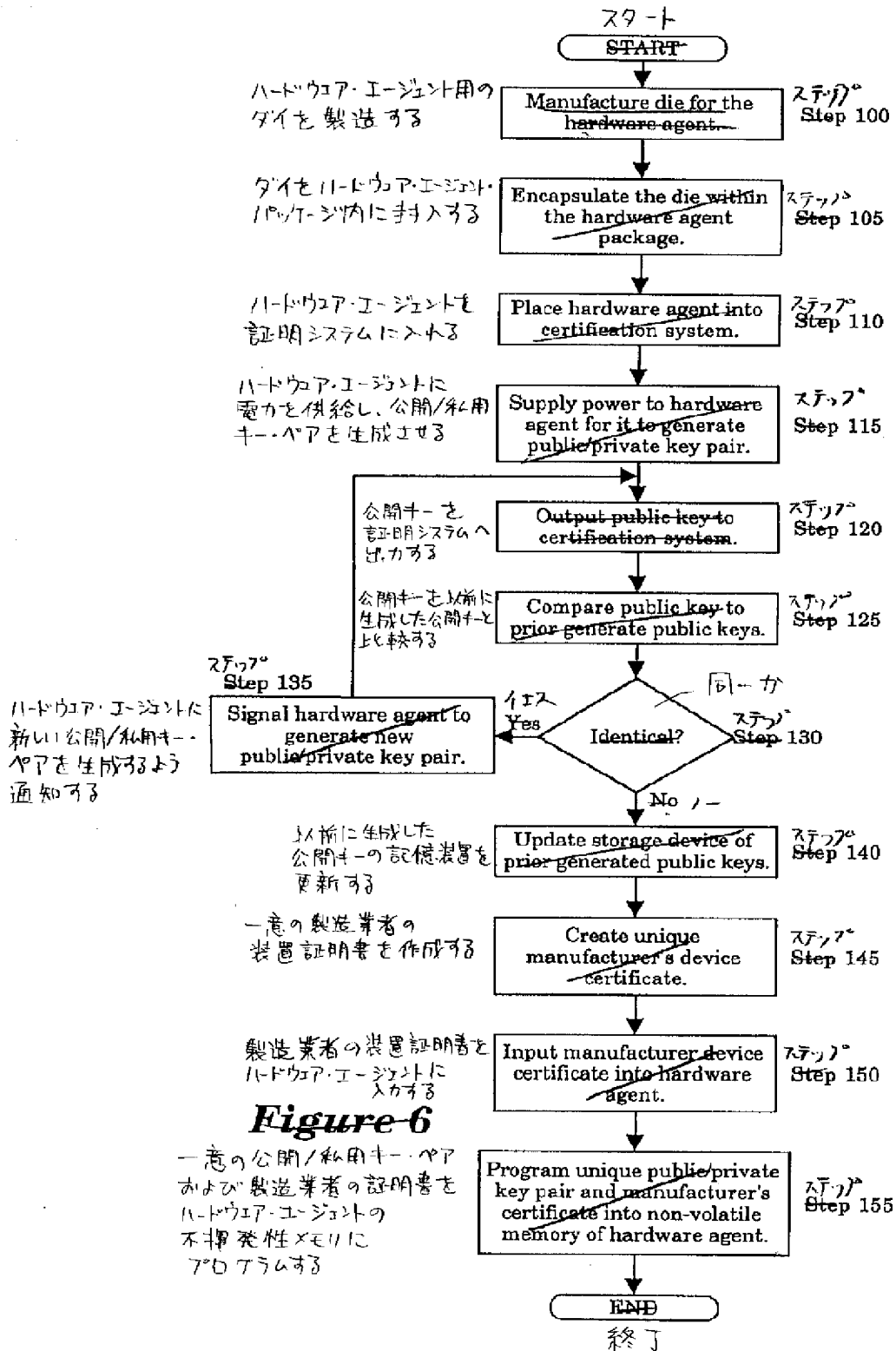


Figure 4

【図5】

**Figure 5**

【図6】



【図7】

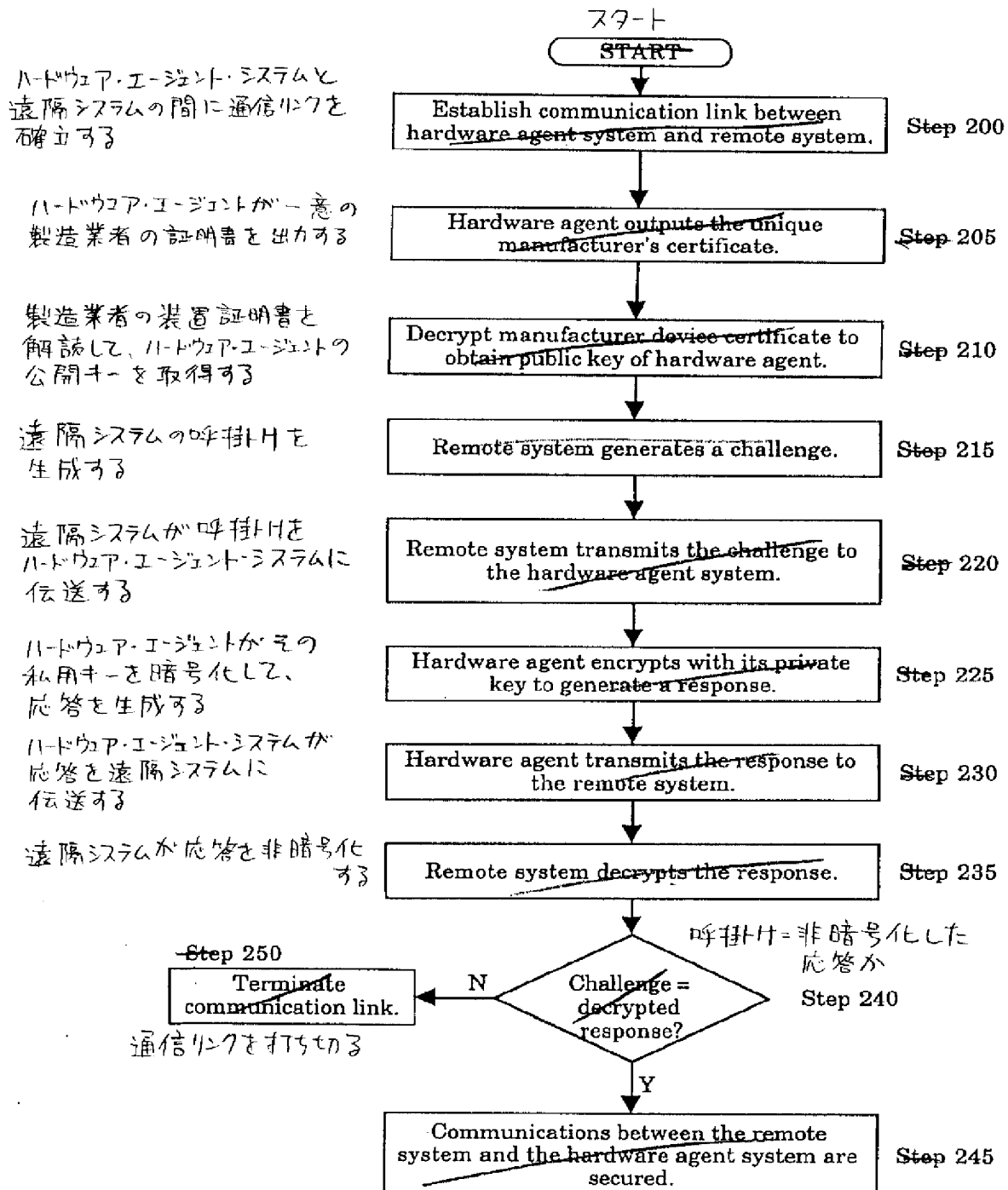


Figure 7

遠隔システムとハードウェア・エージェント・システムとの間の通信は安全保護されている

【図8】

